(c) at each of a plurality of the distributed electronic devices, generating a partial result for the distributed cryptographic computation using at least one of said random values; and

(d) computing a final result for the distributed cryptographic computation using partial results.

2. The method of distributed cryptographic computation as recited by claim 1, wherein said shared values are random keys.

3. The method of distributed cryptographic computation as recited by claim 1, wherein said shared values are derived from a cryptographic protocol.

4. The method of distributed cryptographic computation as recited by claim 1, wherein said shared values are derived cryptographically.

5. The method of distributed cryptographic computation as recited by claim 1, further comprising the step of implementing a re-representation of a function.

6. The method of distributed cryptographic computation as recited by claim 1, wherein said partial results may include incorrect values.

7. The method of distributed cryptographic computation as recited by claim 1, wherein said steps (a)-(d) are performed iteratively.

8. The method of distributed cryptographic computation as recited by claim 7, further comprising changing said shared values after said step of generating an output based on said partial result.

9. The method of distributed cryptographic computation as recited by claim 3, wherein said cryptographic protocol is a cryptographic function involving exponentiation.

10. The method of distributed cryptographic computation as recited by claim 3, wherein said cryptographic protocol is an RSA function.

11. The method of distributed cryptographic computation as recited by claim 1, wherein said shared values are stored in a hardware device in at least one of said distributed electronic devices.

12. A method of distributed cryptographic computation using a cryptographic value shared among a plurality of distributed electronic devices, said method comprising:

(a) selecting a subgroup of devices to perform the distributed cryptographic communication

(b) computing shared values over a known and agreed context, each value being shared among a distinct subset of the subgroup of distributed electronic devices;

(c) at each distributed electronic device of the subgroup, generating a random value using said shared values;

(d) at each device of the subgroup of distributed electronic devices, generating a partial result for the cryptographic computation using a share of the cryptographic value and at least one of said random values; and

(e) computing a final result for the distributed cryptographic computation using partial results.

17. The method of distributed cryptographic computation as recited by claim 1, wherein each of the computed, shared values is shared among a pair of the distributed electronic devices.

18. The method of distributed cryptographic computation as recited by claim 12, wherein each of the computed, of shared values is shared among a pair of the distributed electronic devices.

19. The method of distributed cryptographic computation as recited by claim 1, wherein each computed, shared value is shared among a distinct pair of the distributed electronic devices.

20. The method of distributed cryptographic computation as recited by claim 12, wherein each computed, shared value is shared among a distinct pair of the distributed electronic devices.

21. The method of distributed cryptographic computation as recited by claim 1, wherein each computed, shared value is (a) shared among a distinct subset of distributed electronic devices and (b) used to generate a partial result in a way that permits verification of correctness of a partial result.

B3

22. The method of distributed cryptographic computation as recited by claim 12, wherein each computed, shared value is (a) shared among a distinct subset of distributed electronic devices and (b) used to generate a partial result in a way that permits verification of correctness of a partial result.

23. The method of distributed cryptographic computation as recited by claim 12 wherein the random values depend upon the particular set of devices selected for the subgroup.

24. The method of distributed cryptographic computation as recited by claim 1 wherein the cryptographic computation is based on an argument, and the generated random values are based on said argument.

B4

25. The method of distributed cryptographic computation as recited by claim 12 wherein the cryptographic computation is based on an argument, and the generated random values are based on said argument.